Your web app, protected from the browser, in one tag.

Vaultedo records every attempt to copy, scrape or take your application, marks every screen so a leak traces back to the viewer, and enforces only when you decide. Watch mode is the default.

What you get

Install

One tag, or your AI agent installs it

Paste one tag on the page or one line in the build. Claude Code, Codex, Cursor, VS Code, Gemini CLI and Windsurf can do it over MCP.

Watch

Every attempt recorded, with an alert

View source, saved copies, scraping bursts and a debugger left open are recorded with address, time and device. Alerts are capped.

Trace

An invisible mark on every screen

A forensic code on every screen points back to the viewer and the time when a screenshot leaks. A web page cannot stop a system screenshot; it can make one traceable.

Enforce

Switched on per app, on your word

Right-click, copy, shortcuts, print and framing are refused for the app you choose. Your own console is never blocked.

See

The X-ray

Who opened which screen, after sign-in, where attempts came from by hour and day, and the copies on other addresses. Events are kept for 90 days.

Try it

Attack it yourself first

The website has twelve attacks in four rooms. Outcomes are shown; how the decision is made is not.

What it does not do

- It does not make the code unreadable to a determined person with time.

- It does not stop a camera or an operating-system screenshot.
- It is not end-to-end encryption of your data, and not a replacement for server-side access control.

Start

A 30-day trial at **vaultedo.com**. Watch mode first; enforce when you are sure.

Vaultedo is a solution provided by OPNYX SOLUTIONS. Security: vaultedo.com/security/ · Privacy: vaultedo.com/privacy/